UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,803	08/16/2001	Walter J. Schon	002.0212.01	3342

22895 7590 04/07/2005

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,803	SCHON ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-10,12-20,22-26,28-33,35-39,41-46,48-51 and 53-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-10,12-20,22-26,28-33,35-39,41-46,48-51 and 53-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 70 have been presented for examination. Claims 2, 11, 21, 27, 34, 40, 47 and 52 have been canceled; claims 1, 3, 10, 12, 19, 20, 22, 26, 28, 32, 33, 35, 39, 41, 45, 46, 48, 51, 53 and 56 have been amended in an amendment filed 2/24/2005.

Response to Arguments

2. Applicant's arguments filed on 2/24/2005 have been fully considered but are not persuasive.

3. As per claims 41 and 68, stand rejection under 35 U.S.C. 112, first paragraph, as being not enabled. Applicant argues: "Each encrypted frame is decrypted ... using a private cryptographic key to create a decrypted frame" and "As well, a digital signature is authenticated ... using a public cryptographic key to re-create the cryptographic hash generated from the original framed video content" (see specification Page 16 Lines 20 – 22 and 24 – 27 respectively). Examiner notes Applicant's arguments have been fully considered but are not persuasive. The complete sentence shown in specification is "As well, a digital signature is authenticated using a public cryptographic key to re-create the cryptographic hash generated from the original framed video content". The public / private keys referred to claims 41 and 68 are used solely for the purpose of digital signature due to the dependency of claim language to its associated independent claims 39 and 67 respectively. The hash value is signed (i.e. encryption) with the private key to generate the digital signature and subsequently to re-create the hash

value using a public cryptographic key (i.e. decryption). This is the typical digital signature technique, which also matches the specification (Page 16 Lines 24 – 27). However, it contradicts to what the limitations are claimed in claim 41 and 68, which employ a private key corresponding to the decryption cryptographic key for a digital signature instead of using a public cryptographic key to re-create (i.e. decrypt) the cryptographic hash from the digital signature.

4. As per claim 1 (and related claims), Applicant argues: (a) "Brothers fails to teach or suggest an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium". Examiner notes Applicant's arguments have been fully considered but are not persuasive. Brothers teaches: "the encrypted video frames are stored in memory at the remote station and can be compared to the corresponding frames recorded on the digital tape" (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63: the digital tape is interpreted as transportable storage medium). (b) Applicant further argues: "Brothers does not teach or suggest a decryption module retrieving encrypted frames from a transportable storage and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption". Examiner notes Brothers teaches "played back on a video player that decodes the tape using the public key that is supplied by the trust third party and referenced by the key's identification code" (Brothers: see for example, Column 8 Line 23 – 27). (c) Applicant further argues: "a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video

content in reconstructed form". Examiner notes: "Brothers teaches the decryption unit then passes the decrypted video signal to the viewfinder and external output stage" (Brothers: see for example, Column 7 Line 44 – 47: the video signal must be representing the raw video content in reconstructed form in order to be accessed by the viewfinder and external output stage as taught by Brothers). (d) Applicant further argues: "Brothers does not teach or suggest encrypting and decrypting individual frames and combining the decrypted frames in a playback frame buffer that is described with sufficient precision and detail to establish such subject matter". Examiner notes Brothers teaches recorded each encrypted individual frames into a digital tape and payback / combining the decrypted frames into a substantially continuous video signal (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63, Column 8 Line 23 – 27 and Column 7 Line 44 – 47: all the encryption / decryption frame must be operated in the memory, which can also be referred as memory buffer). Considering the 2nd part of the argument "that is described with sufficient precision and detail to establish such subject matter", Examiner notes Applicant's argument has no merit since the alleged limitation has not been recited into the claim.

5. Furthermore, Applicant argues: "Brothers fails to teach or suggest any form of authentication system or method involving generating an original cryptographic hash of fixed length and then verifying authenticity by generating a verification fixed length cryptographic hash". Examiner notes the 2nd reference Barton is relied upon providing generating an original cryptographic hash of fixed length and then verifying authenticity by generating a verification fixed length cryptographic hash (Barton: see for example,

Column 4 Line 18 – 27, Column 4 Line 1 – 7 and Column 6 Line 37 – 42: using a digital signature through a 16-bit checksum (i.e. hash value)). Applicant further argues: "Neither Brothers nor Barton include any suggestion or incentive that their respective teachings be combined" (Page 23, 3rd Paragraph). Examiner notes the motivation to combine both of the teachings is presented as follows. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barton within the system of Brothers because (a) Brothers discloses the authentication of video frames using the encryption / decryption techniques (Barton: see for example, Column 2 Line 2 – 3), and (b) Barton further teaches providing a cost saving and efficient mechanism for the authentication of video frames by using a digital signature through a 16-bit checksum (i.e. hash value) of video frames (Barton: see for example, Column 4 Line 18 – 27, Column 4 Line 30 and Column 6 Line 37 – 44).

6. Applicant further argues: "Brothers fails to teach or suggest storing encrypted original cryptographic hash as a digital signature on the transportable storage medium". Examiner notes, as stated above, Brothers us relied upon storing encrypted original cryptographic frames on the transportable storage medium (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63), and Barton is relied upon providing a digital signature through a 16-bit checksum of video frames for authentication purpose (Barton: see for example, Column 4 Line 18 – 27, Column 4 Line 30 and Column 6 Line 37 – 44).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 41 and 68 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claim limitation "employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key for a digital signature" is not enabled by the specification according to the disclosure on 2nd Paragraph of Page 16. Besides, the use of private key (instead of public key) to generate the digital signature is the well-known method in the field.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3, 5 – 10, 12, 14 – 18, 20, 22 – 26, 28 – 33, 35 – 39, 41 – 46, 48 – 51 and 53 – 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers (Patent Number: 5799083), in view of Barton (Patent Number: 5912972).

As per claims 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64 and 67, Brothers teaches a system for automatically protecting private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63);

an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium (Brothers: see for example, Column 10 Line 45 – 52 and Column 9 Line 60 – 63: the digital tape is interpreted as transportable storage medium);

a decryption module retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame using a decryption cryptographic key that is verified prior to decryption (Brothers: see for example, Column 8 Line 23 – 27); and

a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form

(Brothers: see for example, Column 7 Line 44 – 47: the video signal must be representing the raw video content in reconstructed form in order to be accessed by the viewfinder and external output stage as taught by Brothers).

However, Brothes does not disclose expressly a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium.

Barton teaches a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium (Barton, see for example, Column 4 Line 18 – 27, Column 4 Line 1 – 7 and Column 6 Line 37 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barton within the system of Brothers because (a) Brothers discloses the authentication of video frames using the encryption / decryption techniques (Barton: see for example, Column 2 Line 2 – 3), and (b) Barton further teaches providing a cost saving and efficient mechanism for the authentication of video frames by using a digital signature through a 16-bit checksum (i.e. hash value) of video frames (Barton: see for example, Column 4 Line 18 – 27, Column 4 Line 1 – 7

and Column 6 Line 37 – 42: using a digital signature through a 16-bit checksum (i.e. hash value)).

Brothers in view of Barton further teaches:

a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash (Barton: see for example, Column 4 Line 18 – 27, Column 4 Line 1 – 7, Column 6 Line 37 – 42, Column 4 Line 30 and Column 6 Line 37 – 44) & (Brothers: see for example, Column 8 Line 23 – 27).

As per claims 3, 12, 22, 28, 35, 41, 58, 61, 65 and 68, Brothers as modified teaches the claimed invention as described above (see claim 1, 10, 20, 26, 33, 39, 57, 60, 64 and 67 respectively). Brothers as modified further teaches providing the encryption and decryption algorithms in use of a public key system (Brothers, see for example, Column 2 Line 14 – 15). Official Notice is taken that the use of an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key for digital signature verification of is one of the well-known methods in the field. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a private key corresponding to the encryption

cryptographic key and a public key corresponding to the decryption cryptographic key for digital signature verification.

As per claims 5, 14, 23, 29, 36 and 42, Brothers as modified teaches the claimed invention as described above (see claim 1, 10, 20, 26, 33 and 39 respectively). Barton further teaches an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key (Barton, see for example, Column 7 Line 19 – 26).

As per claim 6, 15, 48, and 53, see same rationale addressed above in rejecting claim 5.

As per claims 7, 16, 24, 30, 37 and 43, Brothers as modified teaches the claimed invention as described above (see claim 1, 10, 20, 26, 33 and 39 respectively). Brothers as modified further teaches a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key (Brothers, see for example, Column 2 Line 11 – 12).

As per claims 8, 17, 25, 31, 38, 44, 49, 54, 59, 62, 66 and 69, Brothers as modified teaches the claimed invention as described above (see claim 1, 10, 20, 26, 33, 39, 46, 51, 57, 60, 64 and 67 respectively). Brothers as modified further teaches a

removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key (Brothers, see for example, Column C1 Line 59 – 61).

As per claims 9, 18, 50 and 55, Brothers as modified teaches the claimed invention as described above (see claim 8, 17, 49 and 54 respectively). Barton further teaches a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key (Barton, see for example, Column 7 Line 24 – 25).

As per claim 19, 32, 45, 56, 63 and 70, a computer-readable storage medium for performing the methods is provided as taught by Brothers in view of Barton.

9. Claims 4, 13 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers (Patent Number: 5799083), hereinafter referred to as Brothers, in view of Filipi-Martin (Patent Number: US 2002/0112168 A1), hereinafter referred to as Filipi-Martin.

As per claim 4 and 13, Brothers as modified teaches the claimed invention as described above (see claim 1 and 10 respectively). Brothers as modified does not disclose expressly a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames.

Filipi-Martin teaches a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames (Filipi-Martin: see for example, Paragraph [0007] Line 3rd Sentence).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Filipi-Martin within the system of Brothers as modified because Filipi-Martin teaches providing a method so that the validity of the receiver of possessing the decryption key can be assured.

As per claim 19, a computer-readable storage medium for performing the methods is provided as taught by Brothers in view of Barton and Filipi-Martin.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Johns, William L. (U.S. Patent Application Number 09/931,794) discloses "System and Method for Automatically Protecting Private Video Content Using Cryptographic Security for Legacy Systems".

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100